NETWORKING – CLIENT/SERVER WORKPROGRAM CHAPTER 15WP

(FILE NAME ON DISK #3 = IS-WP#10.WPD) ***COMMENTS***

This section is intended to determine the adequacy of the institutions controls over its networking operations. The levels of controls necessary will depend on the degree of reliance the institution places on its network operation. Systems could vary from small isolated LANs to worldwide networks using hardwired and/or vendor-serviced communications services. The networks should be reviewed in consideration of the importance of the information/data to the institution rather than the size of the network installation only. The examiner should document any findings, especially those that do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook.*

Tier I

NETWORK MANAGEMENT

1. If the institution is operating a LAN client/server operation and using a telecommunications system for information transport, describe the system(s) and associated user areas. Use a customer system diagram or create one and determine if the systems are:

   a. Hardwired local or remote client/server operations.

   b. Remote terminal operations using both local and remote client/server operations. Note the transport format including dial-up, leased lines, and value added and, public data networks, etc.

   c. Remote terminal operations using dial-up lines.

   d. Remote terminal operations having file transfer and/or processing capabilities.

   e. Remote client/server operations used for distributed processing and/or print/server operations.

2. Determine if key managers have an adequate segregation of duties and that their skills will enable them to perform their responsibilities.

3. Determine if networked operational systems are addressed adequately in disaster recovery/business contingency planning and testing. Assess the

perceived importance of these systems as compared with the contingency plans.

SECURITY

4. If the institution uses an on-line security system, assess its adequacy and effectiveness.

5. Determine if effective data security policy exists, and if it is being adhered to by:

   a. Discussing the deviations from the published and approved written security policy.

   b. Determining if there is a network security officer review and discussing his/her duties and responsibilities.

   c. Reviewing and determining the authorized access levels allowed within the network operation.

   d. Determining if a password change procedure exists and if it is effective

   e. Determining the composition of passwords (e.g., alphanumeric, nondictionary word validation, etc.).

   f. Determining who has the responsibility for maintaining of the security/password file(s).

   g. Determining whether security violations are monitored and tracked.

6. Arrange with internal audit, the network security officer, systems administrator, or user management to test access controls of selected systems (the examiner should not perform this test directly but rather observe it). Verify the security controls for sign-on, password usage, authorization, and authentification (i.e., read only, update, delete), and log-off. Review the security and/or activity logs that record security violations.

CONTROLS

7. Discuss the data entry controls at the point of origin. If data capture is also obtained through imaging, review – describe the process and associated controls.

Identify the controls in place over the data during input, processing and output activities.

8. If institution is doing any of its own application or systems programming, determine whether there are existing documented policies, procedures, or practices that describe application and systems programming control. Assess whether these procedures are used and are adequate to control new and modified application systems design, development, test, and implementation.

TRAINING

9. Determine whether there is an adequate technical training program for users, operators.

CONCLUSIONS

10. Review the results of work performed in this section and in sections for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

11. Discuss with management:

    a. Violations of law, rulings, regulations,or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

12. Assign rating (See Chapter 5 for additional information).

13. Prepare an index of workpapers for this section of the workprogram.

14. Prepare a separate summary findings worksheet for this section of the workprogram. The summary

should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

15. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

________|_______

Reviewer's Initials

Tier II

Negative responses/determinations should be discussed with management. Their remedy, compensating controls, and your comments must be recorded.

NETWORK MANAGEMENT

1. Obtain an official organization chart and staff position descriptions. Interview management *(*and staff*)* and identify the person(s) responsible for the daily operation of the network (usually the system administrator and security administrator). Determine if the person is qualified, and if there is segregation of duties between persons and any other tasks that they may be assigned/perform. Determine whether there is:

    a. A network system operations manager (sometimes referred to as a systems administrator).

    b. A network security officer (sometimes referred to as a security administrator).

    c. Another person(s) assigned who has specific roles in the control or operational area of the network (include those persons located at remote processing centers).

2. Determine whether system administration and operational procedures are documented and are current and:

    a. Whether the duties and responsibilities assigned to each position and function are clearly defined.

    b. The extent of separation of duties in key functions. Assess whether they are appropriate to the business risks associated with the functions and applications that reside on the system.

3. Determine whether there are written procedures and specific persons assigned, whose responsibilities include:

    a. Initial start-up instructions.

    b. Performance monitoring, operations, and usage.

c. Hardware malfunctions.

d. System security.

e. System maintenance.

f. Applications management.

4. Verify whether the department has current policies, procedures, and standards that are effectively communicated to appropriate personnel and addresses the following areas:

   a. Long- range (strategic) and short-range operating plans that are current and approved by management.

   b. Departmental and institutional policies and procedures.

   c. Each application being run on the network. For commercial applications, determine if there are sufficient license and/or application management controls in place.

   d. System operations procedures, including start-up, shutdown, system shadowing, mirroring, etc.

   e. Tape and/or electronic and optical disk management.

   f. Backup procedures, policies, and offsite storage.

   g. Emergency procedures.

   h. Stock paper and negotiable instrument control procedures.

   i. A contingency/disaster recovery program.

   j. Security procedures and an audit trail program.

5. Determine whether management has developed standards and proceduress defining the levels of information and applications to be classified as sensitive. Determine whether there is a definition of the differences between sensitive, critical, and shared data.

Comments

6. Determine whether management has identified the critical application systems.

7. Determine whether all policies, procedures, and control documents are signed/approved by management.

8. Determine if performance, audit, security, and problem reports are available to management and whether:

   a. They are reviewed by management.

   b. Action has been taken by management and, if so, the type of action.

9. Assess the adequacy of the physical and operational controls of the computer operations area, including access to:

   a. The network, client/servers, and the security, safety, and housekeeping areas of the system.

   b. The network communication system and the security, safety, and housekeeping areas of the component areas.

   c. The terminal devices and the security, safety, and housekeeping areas associated with each unit.

10. Determine the adequacy of controls over operator privilege activities and equipment operations.

11. Determine whether logs are maintained detailing hardware and software problems, and if these logs are reviewed by management.

12. Determine the adequacy of the procedures for reporting and logging equipment failures, maintenance, and repairs, and whether these log reports are reviewed by management.

13. Review the adequacy of reports used by management to monitor computer performance, utilization, and capacity.

14. Determine whether there are maintenance agreements covering all equipment and if not, what is excluded.

SYSTEM OPERATIONS CONTROLS

15. Determine whether procedures exist for problem resolution and:

    a. How they are tracked and their status reported.

    b. If appropriate escalation procedures exist to ensure appropriate response to system problems.

    c. Whether vendor responsibilities are documented in the problem management procedures.

16. Determine if there is a problem resolution log. Review the log and determine if:

    a. Problems recur often.

    b. Resolution timeframes meet management objectives.

    c. Problems represent a system control breakdown.

17. Check for the existence of system maintenance logs for network equipment and servers and determine whether the logs reflect:

    a. An adequate program of periodic preventive maintenance.

    b. Entries for performance capacity monitoring. If not, check to see if the system itself maintains a log.

18. Identify all system-generated logs. Determine if they are being used to track performance, capacity, and transmission quality and verify that procedures exist to:

    a. Periodically review the logs.

    b. Respond to system-identified problems or efficiency degradation.

DISASTER RECOVERY – BUSINESS RESUMPTION CONTINGENCY PLANNING

19. Determine if a written disaster recovery/business resumption contingency plan has been developed for the possible loss of the client/server network, and if it includes:

    a. Securing data files.

    b. Procedures for verifying levels of emergency or processing interruptions (e.g., short-term manual mode).

    c. System application recovery procedures.

    d. Remote storage of data, systems software, documentation, and the recovery plan.

    e. A list of documentation and files maintained offsite.

    f. Procedures to recover from a disaster, including hardware, software, and telecommunications failures.

    g. Provision for securing hardware and supplies.

    h. A location for the backup site.

    i. Approval of management.

20. Assess whether the disaster recovery/business resumption plan has been tested, in simulation, within the past year and:

    a. How often it is tested and how.

    b. Whether the results of the test are documented, and there has been, third-party monitoring of the tests.

21. Determine if policies or procedures exist to ensure the currency of the plan relative to system and/or application changes.

22. Perform an inventory of all items stored at the offsite location and determine the adequacy of the

facility, operation, and backup necessary to recreate files.

SECURITY

23. Verify the physical security provided for servers and communications networking equipment, and that:

    a. All servers are secured (preferably in an area inaccessible to all but authorized systems personnel). Describe how access is:

       - Authorized.

       - Controlled and monitored.

    b. Equipment is provided with physical locking devices or is otherwise properly secured. Determine whether:

       - Keys are properly secured, but accessible to authorized personnel.

       - Duplicate keys are stored and secured properly.

    c. Unrelated equipment and supplies are not stored in the secure area.

24. Verify that the physical security for network distribution equipment is adequate and that:

    a. All major, primary distribution equipment is in controlled access areas.

    b. For secondary distributed equipment (small clusters), it is protected from accidental disconnection or disturbance.

    c. For high risk application/operations, all distribution equipment is protected:

       - From unauthorized physical access.

       - From unauthorized monitoring by use of appropriate sheathing, conduit, or properly installed media.

- By procedures to detect and defeat unauthorized physical access to the distribution system.

d. All workstation distribution cabling and connections are installed properly and secured to prevent accidental disconnection or disturbance.

25. Determine if physical workstation security is adequate and how:

a. Unauthorized removal of workstations and other equipment is prevented.

b. Physical access is controlled and monitored for workstations and other equipment identified as sensitive or high risk.

26. Determine how physical access by vendors to network equipment is controlled and monitored including all equipment in questions 23 through 25 above.

27. Determine whether environmental conditions meet equipment specifications, including:

a. Electrical supply, uninterrupted power supply (UPS) and emergency power and conditioning equipment.

b. Heating ventilation air conditioning (HVAC) systems and controls.

c. Static controls.

28. Determine that fire protection equipment is adequate and appropriate for the system.

29. Determine that fire protection/suppression for onsite stored media is adequate.

30. Determine if onsite storage of all system media is adequate to prevent unauthorized access, including:

a. Server software and backup media.

b. Workstation media.

31. Determine if access to printers and printed output is properly controlled and monitored and:

    a. What physical safeguards exist for sensitive printed output.

    b. What procedures exist for managing the physical distribution of printed output.

DATA SECURITY

32. Must all users on the network enter a logon ID and password to access the network server?

33. Are appropriate password and logon controls in force?

    a. Are the passwords displayed or hidden (nonclear) when they are entered?

    b. Are the passwords encrypted at the workstation before being sent to the server for verification?

    c. Does the system force the user to change passwords regularly? Describe the frequency of change?

    d. Are IDs automatically disabled by the system if passwords are not changed by users?

    e. Does the system prevent passwords from being reused, and are users prevented from changing back to previously used passwords?

    f. Are new users forced to enter a new password on initial logon (passwords pre-expired at first logon)?

    g. Is a minimum length password enforced by the system?

    h. Is there a system to authenticate and preview passwords to prevent common word/name usage (dictionary type password authentication prevention controls)?

i. Are passwords stored as clear text anywhere on the network, including the workstations or in the server?

j. Are user IDs automatically logged off the network after a period of inactivity?

k. Are group or shared IDs and passwords permitted on the network?

l. What compensating controls exist for the use of group or shared IDs and passwords?

m. Do employees sign a corporate systems policy statement acknowledging responsibility for confidentiality or information and secrecy for passwords?

n. Are users informed through guidelines and are they educated about security and establishing passwords

o. Are vendor, contractor, or temporary employee IDs set to pre-expire at the term of their contract?

p. Are vendors, contractors, or temporary employees restricted to appropriate logon days and times?

q. Are vendors, contractors, or temporary employees restricted to specific workstations?

r. Are vendors, contractors, or temporary employees required to sign appropriate nondisclosure statements regarding corporate information to which they may have access?

s. Are IDs disabled after several failed logon attempts? What is the frequency of failed attempts that disables the ID? How long are IDs disabled and how are they restored?

t. Are users notified of the number of prior invalid logon attempts each time they sign onto the system?

34. Are there password logon audit trails that show activity such as:

    a. Logons and logoffs (location, time, and user ID)?

    b. Type of access (dial-up, leased lines, public data networks (Internet, VAN, and etc.)?

    c. Invalid access attempts (location, date, time, ID)?

    d. System expired IDs?

    e. Logoffs due to inactivity?

35. Are audit trails maintained for a reasonable time?

    a. Are they reviewed?

    b. By whom, and how frequently?

    c. What action is taken?

36. Are exception reports produced from audit trails and reviewed by management?

37. Does the network software prevent access by unauthorized users to or from other network services (gateways, FAX, dial-out, WAN, etc.)?

38. Does the network software prevent access by unauthorized users to sensitive system functions such as Security Administration, network monitoring, server console operations, enabling/disabling services, etc.?

39. Are users granted access ONLY to disks, volumes, directories, and files for which they are specifically authorized?

40. Are users able to load and run ONLY those executables for which they are specifically authorized?

41. Identify all software security controls that are not integral to the network's operation system. Evaluate the effectiveness and verify that only

authorized persons can configure or defeat control features.

COMMUNICATIONS SECURITY

42. Determine if internal controls are adequate to prevent:

    a. Incomplete transmission.

    b. Misrouting.

    c. Unauthorized message alteration.

    d. Unauthorized disclosure.

    e. Message duplication.

43. Determine if communications security is built into the communications links on the network, including:

    a. Software packages.

    b. Encryption devices.

    c. Hardware features for the various servers and other processing devices.

44. If the network is connected to outside services or related services through the Internet determine if "firewalls" have been created to centralize access control to-and-from the network and the other service.

45. Determine how microcomputers are connected to each other and other processing entities including:

    a. Modems.

    - Direct dial-up

    - Dial-back.

    b. Hardwired (direct connect).

    c. Leased lines.

    d. Public data networks.

46. Review the adequacy and implementation of controls over the following communications hardware/software processing functions:

    a. Network change control.

    b. Dial-up access.

    c. Network activity logging.

    d. Data encryption.

47. Determine if controls are in place to ensure that data integrity is maintained during data transfer to or from the client/server and other processing entities and identify:

    a. The message authentication procedure.

    b. How the accuracy and completeness of a transmission assured.

    c. For data up and down loading, how batches are identified, screened, and approved on the network.

CONTROLS

48. Review, obtain, or prepare a list of all automated applications currently in use or under development for use on the network client/servers. Identify purchased applications (shrink-wrap and vendor custom contract developed) and those applications that were developed in-house (in-house and contract programmer). Also identify the party(s) responsible for providing maintenance support.

49. For vendor or contract programmer software supplied packages, determine that the following items can be provided by the network administrator. Review the following:

    a. License agreements.

        1. Number of authorized copies or users allowed (site license).

        2. Usage and costs.

b. Maintenance service agreements.

1. Vendor technical support.

2. Allowed modifications that can be made by the institution personnel.

c. User Documentation

1. User operating instructions.

2. Technical documentation.

d. Software acquisition and use policies.

CHANGE CONTROL

50. Determine if procedures exist for operations staff to manage change control.

51. Verify the following:

a. Does the program change process conforms to corporate program change control procedures and standards?

b. Is program change control for the network operation adequate?

c. Are the techniques used to monitor program change control adequate?

d. Does the systems change control procedures take into account the impact to the business, including system availability, user impact, system efficiency, and currency of documentation and manuals?

e. Are there adequate procedures to inform, train, and assist operations staff in the implementation and support of changes in the system.

52. Determine if procedures exist to inform and train users when system changes occur.

53. For network system and utilities, determine if the following are provided:

a. Maintenance information.

1) Technical support group that supports the product.

2) Provisions for receiving operating system fixes, enhancements, and upgrades.

3) Availability of manufacturer's direct support or alternative vendor support.

4) Contract or agreement governing maintenance procedures and services response availability.

b. User Documentation.

1) Is current technical and reference documentation available for operation, administration, and users of the network system software and utilities?

54. Determine if adequate test procedures exist for all changes to the system environment, including those to:

a. Test and implement operating system upgrades, patches, fixes, and enhancements.

b. Test and implement application upgrades, fixes, and enhancements.

c. Test and implement the introduction of new productivity tools and programs.

d. Test and implement changes in the physical environment.

55. Determine if an adequately configured test system exists with appropriate isolation to the “production” environment and:

a. If not, a logical test system exists. Do appropriate controls exist to prevent significant adverse impact to system efficiency or availability.

c. Specific procedures exist to guard against the introduction of “virus” or otherwise tainted executable programs in the test and production environments.

TRAINING AND USER EDUCATION

56. Are policies and procedures in place to ensure adequate technical training of the users, operators, and staff?

57. Does adequate documentation exist for use in training and as reference material for all system and application functions?

58. Are security and control concerns part of the education and training programs for the users, staff, and operators of the system?

59. How are corporate information systems policies communicated to personnel relative to training programs and materials?

60. How are changes to the system accounted for in training and education programs, including documentation and work aids?

61. Proceed to Tier I step 10.

Examiner | Date
_________|________

Reviewer’s Initials